RECEIVED
CENTRAL FAX CENTER
OCT 0 6 2006

REMARKS

No amendments have been made. Claims 1-21 remain pending.

Claim Rejection Under 35 U.S.C. § 103

In the Final Office Action, the Examiner rejected claims 1-21 under 35 U.S.C. 103(a) as being unpatentable over Scott et a. (US 6,484,260) in view of Davis (US 5,568,552), Labaton (US 2002/0191765) and Doub et al. (US 6,594,762). Applicant respectfully traverses the rejection. The applied references fail to disclose or suggest the inventions defined by Applicant's claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

With regard to independent claim 1, Scott in view of Davis, Labaton, and Doub fail to teach or suggest a policy manager component that, during a currently logged-in session of the user associated with the personal digital identifier device, directs at least one of the workstations to blank out a respective screen when a second personal digital identifier device is detected at a location within an envelope until such time as a user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session. Scott in view of Davis, Labaton, and Doub fail to teach or suggest similar elements of independent claims 9 and 17.

In rejecting independent claims 1, 9 and 17, the Examiner correctly recognized that Scott in view of Davis and Labaton failed to teach or suggest these elements. In particular, the Examiner admitted that Scott only discloses a user of a personal digital identifier (PDI) approaching an ATM and being authenticated to access his or her information.[1] The Examiner then further admitted that Scott in view of Davis and Labaton failed to teach or suggest a policy manager component that directs the workstation to blank out the screen during a currently logged-in session of the user associated with a first personal digital identifier device when a second personal digital identifier device is detected at a location within an envelope until such time as the user registered to the second personal digital identifier device is biometrically identified.

[1] Office Action, page 10.

However, the Examiner concludes that Daub teaches these elements and is an obvious combination to Scott in view of Davis and Labaton. In particular, the Examiner states that "Doub et al. discloses a method of wireless authorized remote device 110 authentication in a range distance proximity and a method of denying a display access of personal data/sensitive data to authorized remote device while the authorized remote device is in logged-in session and away from the computer."[2] For support, the Examiner cites col. 1, ll. 12-35, FIG. 1 and col. 4, ll. 26-45 of Doub.

Applicant disagrees with the conclusion of obviousness for a number of reasons. First, the Examiner's own characterization of Doub does not teach Applicant's claim elements that she previously admitted as not taught by the other references. The Examiner admitted that Scott in view of Davis and Labaton failed to teach or suggest a policy manager component that performs the function of actively blanking a workstation screen even during a currently logged-in session of an authorized user when a second personal digital identifier device is detected until such time as the user registered to the second personal digital identifier device is also biometrically identified. In contrast, the Examiner herself characterized Doub as disclosing only "a method of denying a display access of personal data/sensitive data to authorized remote device while the authorized remote device is in logged-in session and away from the computer."

Notably, the Examiner's characterization of Doub makes no reference to detection of a second device at all, let alone during a currently logged-in session of an authorized user associated with a first device. Moreover, the Examiner's characterization of Doub only refers to denying a display access when that authorized user is away from the computer. This is inadequate to teach or discuss blanking a display of a currently logged-in session of an authorized user associated with a first device when a second device is detected. This is prima facie evidence of the deficiency of Doub as teaching such elements.

This inadequacy is borne out in the disclosure of Doub which only describes "enabling a display of an electronic device when the electronic device and a remote device, are located within a transmit range of each other and disabling the display when the electronic device and the remote device are not within the transmit range of each other."[3] Doubs makes very clear that

[2] Office Action, page 10.
[3] Doub et al., Col. 1, ll. 48-52.

disabling of the display only occurs when the electronic device and the remote device are out of transmit range of each other.

Disabling a display when no authorized device is in range, as taught by Doubs, does not provide any basis for blanking a display of a currently logged-in session of an authorized user associated with a first device when a second device is detected. Quite the contrary, the Doubs system teaches handling the situation quite differently.

According to Doubs, a screen is only blanked when the currently authorized deviced is no longer in range. If the device of the authorized user is within range then, according to the teachings of Doubs, the Doubs system does not disable the screen. This entirely contradicts Applicant's claim language. For at least this reason, even if the combination of Scott in view of Davis and Labaton and Daub was made, the resulting system would not include a policy manager component that directs at least one of the workstations to blank out a respective screen of a currently logged-in session of an authorized user when a second personal digital identifier device is detected at a location within an envelope.

Doub does contemplate or discuss the situation where an unauthorized, or second, remote device is detected during a session of an authorized user. Doub explains that "the first authentication code may provide additional security against an unauthorized remote device masquerading as the authorized remote device 110."[4] Doub continues, "If the reply signal does not include the correct first authentication code, the display controller 210 will not enable the display 115."[5] Doub only states that controller 210 will not enable display 115 if the remote device is unauthorized. This, therefore, refers to the situation where the display is already disabled and the only device that responds is an unauthorized device. However, Doub does not contemplate the situation where multiple devices are present, where one of the devices relates to an authorized user that is already logged-in, and a second device is detected that is associated with a user that has not yet authorized.

The Examiner has pointed to no teaching in any of the references, even in combination, that suggest handling the situation where multiple devices are present, one of the devices relates to an authorized user that is already logged-in, and a second device is associated with a user that

[4] Doub et al., Col. 4, ll. 38-40.
[5] Doub et al., Col. 4, ll. 41-43.

has not yet authorized. The combination proposed by the Examiner would not result in a system that blanks out a screen of a logged-in session of an authorized user when a second personal digital identifier device is detected, as required by the independent claims. Instead, the teachings pointed to by the Examiner suggest that the system would enable the screen since the first device is an authorized device and, presumably, within transmit range. In fact, the system suggested by the Examiner would not take any action until the first device is no longer in transmit range, which fails to teach or suggest the features of Applicant's independent claims.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims 1-21 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:

October 6, 2006

By:

Kent Sieffert

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

Name: Kent J. Sieffert
Reg. No.: 41,312